



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,769	12/04/2001	John G. Brainard	RSA-054	3025
23483	7590	04/12/2006	EXAMINER	
		WILMER CUTLER PICKERING HALE AND DORR LLP		CHAI, LONGBIT
		60 STATE STREET	ART UNIT	PAPER NUMBER
		BOSTON, MA 02109	2131	

DATE MAILED: 04/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/010,769	BRAINARD ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 16 March 2006.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-31 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-31 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 04 December 2001 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. Original application contained claims 1 – 31. Claims 15 and 16 have been amended in an amendment filed on 3/16/2006. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 31.

Response to Arguments

1. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.
2. As per claim 1, Applicant argues: "Weiss and Kocher does not teach generating an authentication code by combining the stored secret, the dynamic value, the first generation value, and the PIN because the meaning of the word "combining" is the combination of the secret (K) the dynamic value (T) and the generation value (N) May take place in any order and may use one or more various combination methods. For example, the values (K, T, N) are XOR with each other to arrive at a resulting authentication code; or in another embodiment, the values (K, T, N) are provided as input to a one-way function...". Examiner notes Applicant's argument has no merit since the alleged limitation has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).
3. Applicant asserts: "Weiss does not teach combining any of these values with a first generation value. Examiner notes Kocher is relied upon, besides Weiss, to provide

combining any of these values with a first generation value (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60: a transaction counter is equivalent to a first generation value and each transaction is initiated with a new session of communication that requires authentication. The time interval is equivalent to depth of the counter (generation value) for each cycle length).

4. Applicant asserts: "Kocher does not teach generating an authentication code by combining that transaction counter with any value". Examiner disagrees. Kocher thoroughly teaches a security key update process to securely computing, for example, a message authentication code by combining, at least a transaction counter and a secret value (Kocher: Column 4 Line 39 – 44).
5. Applicant asserts: "Weiss does not teach generating a second generation value responsive to receipt of the PIN". Examiner notes Kocher is relied upon, besides Weiss, to provide generating a second generation value responsive to receipt of the PIN (Kocher: Column 3 Line 54 – 60 and Column 4 Line 33 – 34: a transaction counter is equivalent to a generation value and each transaction counter (including the 2nd generation value) is initiated with a new session of communication requiring the authentication associated with a PIN).
6. Applicant asserts: "Kocher does not teach using a PIN to generate the secret key (or authentication code)". Examiner notes Weiss is relied upon, besides Weiss, using a PIN to generate the secret key (Weiss: Column 5 Line 44 – 49).

7. At last, Applicant argues: "there is no motivation to combine the teaching of Kocher within the system of Weiss". Examiner disagrees and the motivation is presented as follows.

- Weiss discloses a method to prevent externally monitoring attacks to gather repeatedly used the same / fixed secret value correlated to the identification code for accessing to the system resources (Weiss: Column 1 Line 55 – Column 2 Line 2).
- Kocher teaches an enhanced mechanism by providing a fast and more efficient method to eliminate the relatively easily access to someone who misappropriates a secret "fixed" code by dynamically updating the security key during the authentication of the new session communications (Kocher: Column 2 Line 12 – 15, Column 2 Line 40 – 53 and Column 4 Line 43 – 51).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1 – 28 and 30 – 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss (U.S. Patent 4885778), in view of Kocher (U.S. Patent 6539092).

As per claim 1 and 17, Weiss teaches a method for generating an authentication code associated with an entity, the method comprising the steps of:

retrieving a stored secret associated with an entity (Weiss: Column 5 Line 40 – 49: a seed is equivalent to a secret);

determining a dynamic value associated with a time interval (Weiss: Column 2 Line 5 – 15);

receiving a personal identification number (PIN) (Weiss: Column 5 Line 40 – 49);

Weiss does not disclose expressly retrieving a first generation value indicative of a number of previous authentication code generations.

Kocher teaches retrieving a first generation value indicative of a number of previous authentication code generations (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60: a transaction counter is equivalent to a first generation value and each transaction is initiated with a new session of communication that requires authentication. The time interval is equivalent to depth of the counter (generation value) for each cycle length as taught by Kocher).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kocher within the system of Weiss because (a) Weiss discloses a method to prevent externally monitoring attacks to

gather repeatedly used the same / fixed secret value correlated to the identification code for accessing to the system resources (Weiss: Column 1 Line 55 – Column 2 Line 2) and (b) Kocher teaches an enhanced mechanism by providing a fast and more efficient method to eliminate the relatively easily access to someone who misappropriates a secret “fixed” code by dynamically updating the security key during the authentication of the new session communications (Kocher: Column 2 Line 12 – 15, Column 2 Line 40 – 53 and Column 4 Line 43 – 51).

generating an authentication code by combining the stored secret, the dynamic value, the first generation value, and the PIN (Weiss: Column 6 Line 28 – 66; Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60); and

generating a second generation value responsive to receipt of the PIN (Kocher: Column 3 Line 54 – 60 and Column 4 Line 33 – 34 & Weiss: Column 5 Line 20 – 22: a transaction counter is equivalent to a generation value and each transaction counter (including the 2nd generation value) is initiated with a new session of communication requiring the authentication associated with a PIN).

As per claim 2, Weiss as modified teaches receiving verifier information, and wherein the generating step comprises combining the stored secret, the dynamic value, the first generation value, the PIN, and the verifier information (Weiss: Column 10 Line 49 – 60: the time offset is qualified as a verifier information during the authentication).

As per claim 3 and 19, Weiss as modified teaches combining the stored secret and the dynamic value to form a first result; combining the verifier information with the first result to form a second result; and combining the first generation value with the second result (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60; Weiss: Column 6 Line 28 – 66, Column 10 Line 49 – 60 and Column 7 Line 65 – Column 8 Line 17: One of ordinary skill in the art would have expected, at the time the invention was made, the different sequence of combining the presented parameters to perform equally well and as such the combination can occur in any order).

As per claim 4 and 20, Weiss as modified teaches combining the stored secret and the PIN to form a first result; combining the dynamic value with the first result to form a second result; and combining the first generation value with the second result (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60; Weiss: Column 6 Line 28 – 66, Column 10 Line 49 – 60 and Column 7 Line 65 – Column 8 Line 17: One of ordinary skill in the art would have expected, at the time the invention was made, the different sequence of combining the presented parameters to perform equally well and as such the combination can occur in any order).

As per claim 5 and 21, Weiss as modified teaches combining the stored secret and the first generation value to form a first result; combining the dynamic value with the first result to form a second result; and combining the PIN with the second result (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60;

Weiss: Column 6 Line 28 – 66, Column 10 Line 49 – 60 and Column 7 Line 65 – Column 8 Line 17: One of ordinary skill in the art would have expected, at the time the invention was made, the different sequence of combining the presented parameters to perform equally well and as such the combination can occur in any order).

As per claim 6 and 22, Weiss as modified teaches combining the stored secret and the dynamic value to form a first result; and combining the first generation value with the first result (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60; Weiss: Column 6 Line 28 – 66, Column 10 Line 49 – 60 and Column 7 Line 65 – Column 8 Line 17: One of ordinary skill in the art would have expected, at the time the invention was made, the different sequence of combining the presented parameters to perform equally well and as such the combination can occur in any order).

As per claim 7 and 23, Weiss as modified teaches combining the stored secret and the first generation value to form a first result; and combining the dynamic value with the first result (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60; Weiss: Column 6 Line 28 – 66, Column 10 Line 49 – 60 and Column 7 Line 65 – Column 8 Line 17: One of ordinary skill in the art would have expected, at the time the invention was made, the different sequence of combining the presented parameters to perform equally well and as such the combination can occur in any order).

As per claim 8 and 24, Weiss as modified teaches combining the dynamic value and the first generation value to form a first result; and combining the stored secret with the first result (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60; Weiss: Column 6 Line 28 – 66, Column 10 Line 49 – 60 and Column 7 Line 65 – Column 8 Line 17: One of ordinary skill in the art would have expected, at the time the invention was made, the different sequence of combining the presented parameters to perform equally well and as such the combination can occur in any order).

As per claim 9 and 25, Weiss as modified teaches determining a dynamic value responsive to a time-based counter (Weiss: Column 6 Line 47 – 49).

As per claim 10 and 26, Weiss as modified teaches incrementing a generation counter for an authentication code generated during the time interval (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60: a transaction counter is equivalent to a first generation value and each transaction is initiated with a new session of communication that requires authentication. The time interval is equivalent to depth of the counter (generation value) for each cycle length as taught by Kocher).

As per claim 11 and 27, Weiss as modified teaches resetting the generation counter at the start of a second time interval (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60: The time interval is equivalent to depth of the counter (generation counter value) for each cycle length as taught by Kocher).

As per claim 12 and 28, Weiss as modified teaches displaying the authentication code on a display (Weiss: Column 5 Line 59 – 65).

As per claim 13 and 30, Weiss as modified teaches the PIN is retrieved from a data store (Weiss: Column 5 Line 30 – 32).

As per claim 14, Weiss as modified teaches selecting a combination function based on the first generation value (Weiss: Column 6 Line 28 – 66; Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60: the combination function is alternatively determined by the generation value).

As per claim 15, Weiss as modified teaches retrieving a stored secret comprises retrieving one of a plurality of stored secrets based on the first generation value (Weiss: Column 6 Line 28 – 66; Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60: the secret is alternatively determined by the generation value).

As per claim 16 and 31, Weiss as modified teaches retrieving a first generation value indicative of a number of previous code generations within the time interval (Kocher: Column 2 Line 47 – 53, Column 5 Line 4 – 5 and Column 3 Line 54 – 60: a transaction counter is equivalent to a first generation value and each transaction is initiated with a new session of communication that requires authentication. The time

interval is equivalent to depth of the counter (generation value) for each cycle length as taught by Kocher).

As per claim 18, Weiss as modified teaches the PIN subsystem further comprises a keypad (Weiss: Column 5 Line 27 – 30).

3. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss (U.S. Patent 4885778), in view of Kocher (U.S. Patent 6539092), and in view of Koopman et. Al. (U.S. Patent 5377270).

As per claim 29, Weiss as modified does not disclose expressly the generation value subsystem changes the generation value upon activation of a button.

Koopman teaches the generation value subsystem changes the generation value upon activation of a button (Koopman: Column 11 Line 36 – 38).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Koopman within the system of Weiss as modified because Koopman teaches providing an improved remote operating system with an enhanced security mechanism that is extremely difficult to breach by analysis (Koopman: Column 2 Line 42 – 44).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131


LBC

CHRISTOPHER REVAK
PRIMARY EXAMINER

Cell 412106